Two variants of the support problem for products of abelian varieties and tori

Antonella Perucca

Abstract

Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-rational points on G. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$. Then there exist a K-endomorphism ϕ of G and a non-zero integer c such that $\phi(P) = cQ$. Furthermore, we are able to prove the above result with weaker assumptions: instead of comparing the order of the points we only compare the radical of the order (radical support problem) or the ℓ-adic valuation of the order for some fixed rational prime ℓ (ℓ-adic support problem).

1 Introduction

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point on G and let ϕ be a K-endomorphism of G. Then for all but finitely many primes $\mathfrak{p}$ of K the order of $(\phi(R) \bmod \mathfrak{p})$ divides the order of $(R \bmod \mathfrak{p})$. The support problem is concerned with the converse: what can we say about two K-rational points P and Q satisfying the following condition?

(SP) The order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

This question was first studied in [5], [7] and [4]. Larsen solved the support problem for abelian varieties by showing that there exist a K-endomorphism ϕ and a non-zero integer c such that $\phi(P) = cQ$ ([9, Theorem 1]). In general, one can not take $c = 1$ even if P and Q have infinite order ([9, Proposition 2]).

We study two variants of the support problem, which we call respectively *ℓ-adic support problem* and *radical support problem*. We require weaker conditions on the points:

(LSP) Fix a rational prime ℓ and suppose that the ℓ-adic valuation of the order of $(Q \bmod \mathfrak{p})$ is less than or equal to the ℓ-adic valuation of the order of $(P \bmod \mathfrak{p})$, for all but finitely many primes $\mathfrak{p}$ of K.

(RSP) Fix an infinite set S of rational primes and suppose that for every ℓ in S the order of $(Q \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{p})$ is coprime to ℓ, for all but finitely many primes $\mathfrak{p}$ of K.

We strengthen Larsen's result on the support problem by proving the following:

Main Theorem. *Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-rational points on G. Suppose that P and Q satisfy condition (LSP) or condition (RSP). Then there exist a K-endomorphism ϕ of G and a non-zero integer c such that $\phi(P) = cQ$.*

For abelian varieties, our result has an alternative proof: the proof by Larsen of [9, Theorem 1] only requires condition (RSP); the proof by Wittenberg of [9, Theorem 1] inspired from [10] only requires condition (LSP), see [15]. For the multiplicative group or simple abelian varieties and assuming condition (LSP), equivalent results were proven respectively by Khare in [6, Proposition 3] and by Barańczuk in [1, Theorem 8.2].

Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be points in $G(K)$ satisfying one of the conditions above. Let c be the least positive integer such that cQ belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by P. We prove the following:

Assuming condition (SP), c divides a non-zero integer m which depends only on G and K. For abelian varieties this result has an alternative proof by Larsen, see [10].

Assuming condition (LSP), the ℓ-adic valuation of c is less than or equal to the ℓ-adic valuation of a non-zero integer m which depends only on G and K (notice that m does not depend on ℓ).

Assuming condition (RSP), there exists a non-zero integer m depending only on G and K such that the following holds: for every ℓ in S coprime to m the ℓ-adic valuation of c is zero.

See section 4 for more results concerning c under conditions (SP), (LSP) and (RSP) respectively.

Finally we discuss the *multilinear support problem*, which is a variant of the support problem introduced by Barańczuk in [1]. The points P and Q are replaced by n-tuples of points and the following condition is required:

(MSP) Suppose that for all but finitely many primes $\mathfrak{p}$ of K and for all positive integers $m_1, \ldots, m_n$ the point $(m_1Q_1 + \ldots + m_nQ_n \bmod \mathfrak{p})$ is zero whenever the point $(m_1P_1 + \ldots + m_nP_n \bmod \mathfrak{p})$ is zero.

This condition is stronger than requiring condition (SP) on each pair of points (P_i, Q_i) so there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. One would

like to prove that ϕ_i and ϕ_j are related for $i \neq j$. This is true if the endomorphism ring is $\mathbb{Z}$ (see [1]) but in general ϕ_i and ϕ_j are not related for $i \neq j$, see section 5. Another multilinear condition has recently been considered by Barańczuk, see [2].

2 Preliminaries

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point on G and call G_R the smallest algebraic K-subgroup of G containing R. Write G_R^0 for the connected component of the identity of G_R and write n_R for the number of connected components of G_R.

We say that R is *independent* if R is non-zero and $G_R = G$. The point R is independent in G if and only if R is independent in $G \times_K \bar{K}$. Furthermore, R is independent in G if and only if R is non-zero and the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free. See [13, Section 2].

Proposition 1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point on G. Then n_R divides a non-zero integer which depends only on G and K.*

Proof. Write $G = A \times T$ and $R = (R_A, R_T)$. Since $G_R \subseteq G_{R_A} \times G_{R_T}$, we know that G_R^0 is the product of an abelian subvariety A' of $G_{R_A}^0$ and a subtorus T' of $G_{R_T}^0$ (see [13, Proposition 5]). We have $A' = G_{R_A}^0$ because A' contains a non-zero multiple of R_A. Analogously we have $T' = G_{R_T}^0$. So $G_R^0 = G_{R_A}^0 \times G_{R_T}^0$ hence n_R divides the number of connected components of $G_{R_A} \times G_{R_T}$. Then it suffices to prove the statement for A and for T respectively.

For A the statement is proven in [12, Lemma 2.2.4]. Now we prove the statement for T: we reduce at once to the case $T = \mathbb{G}_m^n$. Write $R = (R_1, \ldots, R_n)$ and let e be the exponent of $\mathbb{G}_m(K)_{tors}$. Since n_R divides e times n_{eR}, we reduce to the case where $R_1, \ldots, R_n$ generate a torsion-free subgroup of $\mathbb{G}_m(K)$. We conclude by proving that in this case $n_R = 1$. We may clearly assume that R is non-zero. Fix a rational prime ℓ. Remark that $R_1, \ldots, R_n$ generate a free subgroup of $\mathbb{G}_m(K)$. By choosing a basis for this subgroup, we find an integer $s \geq 1$ and a point R' independent in $\mathbb{G}_m^s$ such that $\mathrm{ord}(R \bmod \mathfrak{p}) = \mathrm{ord}(R' \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. By [13, Proposition 12] there exist infinitely many primes $\mathfrak{p}$ such that $v_\ell[\mathrm{ord}(R' \bmod \mathfrak{p})] = 0$. Then for infinitely many primes $\mathfrak{p}$ we have $v_\ell[\mathrm{ord}(R \bmod \mathfrak{p})] = 0$. By [13, Main Theorem], it follows that $v_\ell(n_R) = 0$. □

Lemma 2. *Let G be the product of an abelian variety and a torus defined over a number field K. Let L be a finite Galois extension of K of degree d. Let P and Q be K-rational points on G. If Q belongs to $\mathrm{End}_L G \cdot P$ then dQ belongs to $\mathrm{End}_K G \cdot P$.*

Proof. Suppose that there exists ψ in $\mathrm{End}_L G$ such that $\psi(P) = Q$. Set $\phi = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi^\sigma$.

Then ϕ is in $\mathrm{End}_K G$ and we have:

$$\phi(P) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi^\sigma(P) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi(P)^\sigma = \sum_{\sigma \in \mathrm{Gal}(L/K)} Q^\sigma = dQ.$$

□

Lemma 3. *Let A and B be products of an abelian variety and a torus defined over a number field K. Let α be an isogeny in $\mathrm{Hom}_K(A, B)$ and let d be the exponent of the kernel of α (which divides the degree of α). Let R be a K-rational point on A. For all but finitely many primes $\mathfrak{p}$ of K the following holds: the order of $(dR \bmod \mathfrak{p})$ divides the order of $(\alpha(R) \bmod \mathfrak{p})$.*

Proof. For every ψ in $\mathrm{Hom}_K(B, A)$ and for every point W in $B(K)$ the following holds: the order of $(\psi(W) \bmod \mathfrak{p})$ divides the order of $(W \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. Call $\hat{\alpha}$ the isogeny in $\mathrm{Hom}_K(B, A)$ such that $\hat{\alpha} \circ \alpha = [d]$. The statement follows by applying the first assertion to $\psi = \hat{\alpha}$ and $W = \alpha(R)$. □

Lemma 4. *Let K be a number field. Let $I = \{1, \ldots, n\}$. For every $i \in I$ let B_i be the product of an abelian variety and a torus defined over K. Suppose that for $i \neq j$ either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. Let $H = \prod_{j \in J} B_j$ for some subset J of I and let R be a point in $H(K)$ which is independent in H. Let W be a point in $B_n(K)$. Then if (R, W) is not independent in $H \times B_n$ there exists a non-zero f in $\mathrm{End}_K B_n$ such that $f(W)$ belongs to $\mathrm{Hom}_K(H, B_n) \cdot R$.*

Proof. We know that there exists a non-zero F in $\mathrm{End}_K(H \times B_n)$ such that $F(R, W) = 0$. Write $F = (F_1, F_2)$ in the decomposition

$$\mathrm{End}_K(H \times B_n) = \mathrm{Hom}_K(H, H \times B_n) \times \mathrm{Hom}_K(B_n, H \times B_n).$$

We then have $F_1(R) + F_2(W) = F(R, W) = 0$.

Since $F \neq 0$ there exists a factor B_m of $H \times B_n$ such that $\pi_m \circ F \neq 0$ where π_m is the projection of $H \times B_n$ onto B_m. Now we prove that $\pi_m \circ F_2 \neq 0$. Suppose not. Then we must have $\pi_m \circ F_1 \neq 0$. If B_n is not equal to any factor of H and $B_m = B_n$ we have $\mathrm{Hom}_K(H, B_m) = \{0\}$ hence $\pi_m \circ F_1 = 0$, contradiction. So we may assume that there is an inclusion map i from B_m to H. We have $i \circ \pi_m \circ F_1 \neq 0$ and $i \circ \pi_m \circ F_1(R) = -i \circ \pi_m \circ F_2(W) = 0$, which contradicts the fact that R is independent in H.

Since $\pi_m \circ F_2 \neq 0$, we have $\mathrm{Hom}_K(B_n, B_m) \neq \{0\}$ hence $B_m = B_n$. Call $f = \pi_m \circ F_2$. Then f is a non-zero element of $\mathrm{End}_K B_n$ and we have $f(W) = -\pi_m \circ F_1(R)$ hence $f(W)$ belongs to $\mathrm{Hom}_K(H, B_n) \cdot R$. □

Lemma 5. *Let K be a number field and let $I = \{1, \ldots, n\}$. Let $G = \prod_{i \in I} B_i$ where for every i B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for $i \neq j$ either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. Let $P = (P_1, \ldots, P_n)$ be a point on $G(K)$ of infinite order. Then*

there exist a subset $J = \{j_1, \ldots, j_s\}$ of I and a non-zero integer d such that the point $P' = (P_{j_1}, \ldots, P_{j_s})$ is independent in $G' = \prod_{j\in J} B_j$ and such that for all but finitely many primes $\mathfrak{p}$ of K the order of $(P \bmod \mathfrak{p})$ divides d times the order of $(P' \bmod \mathfrak{p})$.

Proof. We prove the statement by induction on n. If $n = 1$, the point P_1 is independent in B_1 so take $J = \{1\}$, $d = 1$. Now we prove the inductive step. Let $P = (P_1, \ldots, P_n)$ and set $\tilde{P} = (P_1, \ldots, P_{n-1})$. If $\tilde{P}$ is a torsion point then P_n is independent in B_n and we easily conclude. So assume that $\tilde{P}$ has infinite order and let $\tilde{J}$, $\tilde{d}$, $\tilde{P}'$ and $\tilde{G}'$ be as in the statement. If the point $(\tilde{P}', P_n)$ is independent in $\tilde{G}' \times B_n$ take $J = \tilde{J} \cup \{n\}$ and $d = \tilde{d}$. Otherwise by Lemma 4 there exists a non-zero f in $\mathrm{End}_K B_n$ such that $f(P_n)$ is in $\mathrm{Hom}_K(\tilde{G}', B_n) \cdot \tilde{P}'$.

Since f is an isogeny, there exist $\hat{f}$ in $\mathrm{End}_K B_n$ and a non-zero integer r such that $[r] = \hat{f} \circ f$. Consequently rP_n belongs to $\mathrm{Hom}_K(\tilde{G}', B_n) \cdot \tilde{P}'$ and so we can take $J = \tilde{J}$ and $d = \mathrm{l.c.m.}(\tilde{d}, r)$. □

Lemma 6. *[Proposition 2, Appendix of [3]] Let A be an abelian variety defined over a number field K. There exists a non-zero integer t such that the following holds: for every K-rational point R on A there exists an abelian subvariety Z of A defined over K such that $G_R^0 + Z = A$ and $G_R^0 \cap Z$ has order dividing t.*

The previous lemma can also be found in [14, Proposition 5.1].

3 The proof of the Main Theorem

Lemma 7. *Let A and B be products of an abelian variety and a torus defined over a number field K and K-isogenous. If the Main Theorem is true for B, then it is true for A.*

Proof. Suppose that the Main Theorem holds for B. Let α be a K-isogeny from A to B, call d the degree of α and call $\hat{\alpha}$ the isogeny in $\mathrm{Hom}_K(B, A)$ satisfying $\hat{\alpha} \circ \alpha = [d]$. Because of Lemma 3, if P and Q satisfy condition (LSP) then for all but finitely many primes $\mathfrak{p}$ of K we have:

$$v_\ell[\mathrm{ord}(\alpha(P) \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(dP \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(dQ \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(\alpha(dQ) \bmod \mathfrak{p})].$$

So $\alpha(P)$ and $\alpha(dQ)$ satisfy condition (LSP). By Lemma 3, if P and Q satisfy condition (RSP) then $\alpha(P)$ and $\alpha(Q)$ satisfy condition (RSP) for the subset of S consisting of the primes coprime to d. We deduce that

$$\psi\big(\alpha(P)\big) = r\big(\alpha(dQ)\big)$$

where ψ is in $\mathrm{End}_K B$ and r is a non-zero integer. Set $\phi = \hat{\alpha} \circ \psi \circ \alpha$, $c = rd^2$. Then ϕ is in $\mathrm{End}_K A$, c is a non-zero integer and we have:

$$\phi\big(P\big) = \hat{\alpha} \circ \psi \circ \alpha\big(P\big) = \hat{\alpha} \circ [r] \circ \alpha\big(dQ\big) = rd^2Q = cQ.$$

□

Proof of the Main Theorem.
First step. We reduce to prove the theorem for $G = \prod_{i\in I} B_i$ where for every i the factor B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for $i \neq j$ either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. To accomplish this, it suffices to combine two things: the statement holds for G if it holds for $G \times_K L$, where L is a finite Galois extension of K; the statement holds for G if it holds for $\alpha(G)$ where α is a K-isogeny. The first assertion is a consequence of Lemma 2. The second assertion is proven in Lemma 7.
Second step. Let $G = \prod_{i\in I} B_i$ and write $P = (P_1, \ldots, P_n)$, $Q = (Q_1, \ldots, Q_n)$. Without loss of generality we may replace Q by $(Q_1, 0, \ldots, 0)$.
We may assume that Q has infinite order (otherwise take $\phi = 0$ and $c = \mathrm{ord}\, Q$). Then we may assume that also P has infinite order. Otherwise, let ℓ be either the prime of condition (LSP) or a prime of S coprime to $\mathrm{ord}(P)$. We find a contradiction by [13, Corollary 14] since there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] > v_\ell[\mathrm{ord}(P)]$.
Third step. Apply Lemma 5 to P and let J, d, P', G' be as in Lemma 5. Since P' is a projection of P, it suffices to prove that there exist ψ in $\mathrm{Hom}_K(G', B_1)$ and a non-zero integer c such that $\psi(P') = cQ_1$.
Fourth step. The point (P', Q_1) is not independent in $G' \times B_1$. Otherwise, let ℓ be either the prime of condition (LSP) or a prime of S coprime to d and apply [13, Proposition 12]. There exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})] = 0$ and $v_\ell[\mathrm{ord}(Q_1 \bmod \mathfrak{p})] = v_\ell(d) + 1$. We find a contradiction since by definition of d we may assume that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \leq v_\ell(d) + v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})]$.
Fifth step. By definition P' is independent in G' so we can apply Lemma 4 to the points P' and Q_1. Then since (P', Q_1) is not independent in $G' \times B_1$ there exists a non-zero f in $\mathrm{End}_K B_1$ such that $f(Q_1)$ belongs to $\mathrm{Hom}_K(G', B_1) \cdot P'$. Since f is an isogeny, there exist $\hat{f}$ in $\mathrm{End}_K B_1$ and a non-zero integer c such that $[c] = \hat{f} \circ f$. Consequently cQ_1 belongs to $\mathrm{Hom}_K(G', B_1) \cdot P'$. □

The following corollary is the analogue to [9, Corollary 6].

Corollary 8. *Let G_1 and G_2 be products of an abelian variety and a torus defined over a number field K. Let P and Q be K-rational points respectively on G_1 and G_2 satisfying condition (LSP) or condition (RSP). Then there exist ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and a non-zero integer c such that $\phi(P) = cQ$.*

Proof. Apply the Main Theorem to $G_1 \times G_2$ and the points $(P, 0)$ and $(0, Q)$. □

4 On the integer c of the Main Theorem

The following proposition is the generalization of a result by Khare and Prasad ([8, Theorem 1]).

Proposition 9. *Under the assumptions of Corollary 8 and if the point P is independent in G_1, one can take c coprime to ℓ under condition (LSP) and coprime to every ℓ in S under condition (RSP).*

Proof. We have $\phi P = cQ$ for some ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and some non-zero integer c. Let ℓ be either the prime of condition (LSP) or a fixed prime of S. By iteration, it suffices to prove that if c is divisible by ℓ there exists ψ in $\mathrm{Hom}_K(G_1, G_2)$ such that $\psi P = \frac{c}{\ell}Q$. So suppose that c is divisible by ℓ. Let P' be a point in $G_1(\bar{K})$ such that $\ell P' = P$. We then have $\phi(P') = \frac{c}{\ell}Q + Z$ for some Z in $G_2[\ell]$. Write L for a finite extension of K over which $G_1[\ell]$ is split and where P' is defined. Notice that P' is also independent in G_1. The condition of Corollary 8 clearly implies that for all but finitely many primes $\mathfrak{q}$ of L the order of $(Q \bmod \mathfrak{q})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{q})$ is coprime to ℓ.

First we prove that $\phi = [\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Suppose not and then let T be a point in $G_1[\ell] \setminus \ker(\phi)$.

Suppose that $\phi(T) \neq Z$. By [13, Proposition 11] there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P' - T \bmod \mathfrak{q})] = 0$. We deduce that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$ and that the point $(\phi(P') - \phi(T) \bmod \mathfrak{q})$ has order coprime to ℓ. Then

$$r_\mathfrak{q}\phi(T) = r_\mathfrak{q}\phi(P') = r_\mathfrak{q}(\frac{c}{\ell}Q + Z) \ (\mathrm{mod}\,\mathfrak{q})$$

for some integer $r_\mathfrak{q}$ coprime to ℓ. Therefore

$$r_\mathfrak{q}\frac{c}{\ell}Q = r_\mathfrak{q}(\phi(T) - Z) \ (\mathrm{mod}\,\mathfrak{q}).$$

By discarding finitely many primes $\mathfrak{q}$, we may assume that the order of $(\phi(T) - Z \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we find a contradiction.

Now suppose that $\phi(T) = Z$. Then $\phi(P') = \frac{c}{\ell}Q + \phi(T)$. By [13, Proposition 11] there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P' \bmod \mathfrak{q})] = 0$. Then $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$. By discarding finitely many primes $\mathfrak{q}$, we may assume that the order of $(\phi(T) \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we find a contradiction.

So we can factor ϕ as $[\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Then $\psi(P) = \frac{c}{\ell}Q + T'$ for some T' in $G_2[\ell]$. It suffices to prove that $T' = 0$. By [13, Proposition 12], there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$. If $T' \neq 0$, we may assume that the order of $(T' \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we have a contradiction. □

Proposition 10. *Under the assumptions of the Main Theorem, let c be the least positive integer such that cQ belongs to $\mathrm{End}_K G \cdot P$. If condition (LSP) holds then $v_\ell(c) \leq v_\ell(m)$ for some non-zero integer m depending only on G and K. If condition (RSP) holds then $v_\ell(c) = 0$ for every ℓ in S coprime to m, for some non-zero integer m depending only on G and K.*

Proof. We first reduce to the case $G = A \times T$ where A is an abelian variety and $T = \mathbb{G}_m^n$. It suffices to show that the statement holds for G if it holds for $G \times_K L$ where L is a finite Galois extension of K. This can be deduced from the proof of Lemma 2: if m is as in the statement for $G \times_K L$ then for G one can take $[L : K]m$.

We reduce to the case where G_P is connected. By Proposition 1, n_P divides an integer h depending only on G and K. We can then replace P and Q with hP and hQ.

If P is zero then from [13, Corollary 14] we immediately deduce that Q is a torsion point. In this case c divides the exponent of $G(K)_{tors}$.

Now we assume that G_P is connected and that P has infinite order. By [13, Proposition 5], we have $G_P = A' \times T'$ where A' is an abelian subvariety of A and T' is a sub-torus of $\mathbb{G}_m^n$. Since P is independent in G_P, from Proposition 9 it follows that there exist ψ in $\mathrm{Hom}_K(G_P, G)$ and an integer r coprime to ℓ (respectively to every prime of S) such that $\psi(P) = rQ$.

Write $P = (P_A, P_T)$ and remark that $A' = G_{P_A}$ (see the proof of Proposition 1). Apply Lemma 6 to P_A. Let Z and t be as in Lemma 6. Then the map

$$j : A' \times Z \to A\,;\ (x, y) \mapsto x + y.$$

is a K-isogeny in $\mathrm{Hom}_K(A' \times Z, A)$ of degree dividing t. Call $\hat{\jmath}$ the isogeny in $\mathrm{Hom}_K(A, A' \times Z)$ satisfying $\hat{\jmath} \circ j = [t]$. We have:

$$\hat{\jmath}\big(P_A\big) = \hat{\jmath} \circ j\big((P_A, 0)\big) = (tP_A, 0).$$

Then there is an element π_A in $\mathrm{Hom}_K(A, A')$ mapping P_A to tP_A. Since T' is a direct factor of T, there exists π_T in $\mathrm{Hom}_K(T, T')$ such that $\pi_T(P_T) = tP_T$. Let Π be $\pi_A \times \pi_T$. Then Π is in $\mathrm{Hom}_K(G, G_P)$ and $\Pi(P) = tP$. The map $\phi = \psi \circ \Pi$ is in $\mathrm{End}_K G$ and we have $\phi(P) = rtQ$.

Since r is coprime to ℓ (respectively to every prime of S) and t depends only on G and K, this concludes the proof. □

Unless $G(K)$ is finite, one clearly cannot bound $v_p(c)$ for any rational prime p different from ℓ (assuming condition (LSP)) or not in S (assuming condition (RSP)).

Assuming condition (LSP), a straightforward adaptation of [9, Proposition 2] shows that in general one cannot take c coprime to ℓ even if P and Q have infinite order.

For a split torus or for an abelian variety and assuming condition (RSP), one cannot in general bound $v_\ell(c)$ for every ℓ in S:

Example 11. Let ℓ be a rational prime. Let G be either the multiplicative group or an elliptic curve without complex multiplication defined over a number field K. Suppose that $G(K)$ contains a point R of infinite order and a torsion point T of order ℓ. Consider the points $P = (\ell^h R, T)$ and $Q = (R, 0)$ on G^2, for some fixed h in $\mathbb{N}$. Then the points P and Q satisfy condition (RSP) where S is the set of all primes but one has to take c such that

$v_\ell(c) \geq h$. By varying h, we see at once that that one cannot bound $v_\ell(c)$ with a constant depending only on G and K.

Proposition 12. *In the Main Theorem, assuming condition (LSP) and if G is a split torus then one can take c coprime to ℓ.*

Proof. We may assume that $G = \mathbb{G}_m^n$. Recall that $\mathbb{G}_m[a] \simeq \mathbb{Z}/a\mathbb{Z}$ for every $a \geq 1$. Without loss of generality we may assume that $Q = (Q_1, 0, \ldots, 0)$. If P is a torsion point then (because of $\phi(P) = cQ$) Q_1 is also a torsion point and the statement easily follows from condition (LSP). Now assume that P has infinite order. Since $\mathrm{End}_K \mathbb{G}_m \simeq \mathbb{Z}$, we may assume that P is of the following form:

$$P = (R_1, \ldots, R_h, T, 0, \ldots, 0)$$

where the point $(R_1, \ldots, R_h)$ is independent in $\mathbb{G}_m^h$, $h \geq 1$ and T is a torsion point. Call t the ℓ-adic valuation of the order of T.

We have

$$aT + \sum_{i=1}^{h} a_i R_i = cQ_1 \tag{1}$$

for some $a, a_1, \ldots, a_h$ in $\mathbb{Z}$ and for some non-zero integer c. Suppose that c is divisible by ℓ. It suffices to find an expression analogous to (1) where c is replaced by $\frac{c}{\ell}$ and we conclude by iteration.

Now we prove that a is divisible by ℓ. Suppose not. We may clearly assume that $t \neq 0$, otherwise we can multiply every coefficient of (1) by an integer coprime to ℓ and replace a by zero. By [13, Proposition 12] there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every i. We may assume that $v_\ell[\mathrm{ord}(T \bmod \mathfrak{p})] = t$. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq t + 1$ and that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = t$ so we find a contradiction.

Without loss of generality we prove that a_h is divisible by ℓ. Suppose not. The point $(R_1, \ldots, R_{h-1}, a_h R_h + aT)$ is independent in $\mathbb{G}_m^h$. Thus by [13, Proposition 12] there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every $i \neq h$ and $v_\ell[\mathrm{ord}(a_h R_h + aT \bmod \mathfrak{p})] = t + 1$. We easily deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq t + 2$ and that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = t + 1$, contradiction.

Now we can write

$$\frac{a}{\ell} T + \sum_{i=1}^{m} \frac{a_i}{\ell} R_i = \frac{c}{\ell} Q_1 + W$$

where W is in $\mathbb{G}_m[\ell]$.

If $t \geq 1$ then W is a multiple of T and we conclude. If $W = 0$ we also conclude. Now suppose that $t = 0$ and $W \neq 0$. By [13, Proposition 12] there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every i. We may assume that the order of $(W \bmod \mathfrak{p})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = 0$ and $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq 1$, a

contradiction. □

By the previous proposition and Lemma 2, assuming condition (LSP) for a torus one can take c such that $v_\ell(c) \leq v_\ell(d)$ where d is the degree of a finite Galois extension of K where the torus splits. In particular, if G is a 1-dimensional torus one can take c coprime to ℓ (since every endomorphism is defined over K).

We may weaken condition (LSP) in the Main Theorem as follows: there exists an integer $d \geq 0$ such that for all but finitely many primes $\mathfrak{p}$ of K $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})]$ is greater than or equal to $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] - d$. Indeed, it is immediate to see that P and $\ell^d Q$ satisfy condition (LSP).

Notice that the set S in condition (RSP) needs in general to be infinite:

Example 13. Let S be a finite family of prime numbers and let m be the product of the primes in S. Let G be either the multiplicative group or an elliptic curve without complex multiplication defined over a number field K. Suppose that $G(K)$ contains a torsion point T of order m and that the rank of $G(K)$ is greater than 1. Then let (R, W) be a point in $G^2(K)$ which is independent. Consider the points $P = (R, T)$, $Q = (W, 0)$ in $G^2(K)$. The order of P is a multiple of m for all but finitely many primes $\mathfrak{p}$ of K hence the points P and Q satisfy condition (RSP) for the set S. Nevertheless, no non-zero multiple of Q lies in the left $\mathrm{End}_K G^2$-submodule of $G^2(K)$ generated by P.

Now suppose that condition (SP) holds. In general one can not take $c = 1$ even if P and Q have infinite order ([9, Proposition 2]). As a consequence of Proposition 9, one can take $c = 1$ if P is independent in G. This is the generalization of a result by Khare and Prasad ([8, Theorem 1]). As a consequence of Proposition 10, one can take c such that it divides a constant depending only on G and K. This was known for abelian varieties, see [10, Corollary 4.4 and Theorem 5.2] by Larsen. More precisely, Larsen proved that for abelian varieties one can take c dividing the exponent of $G(K)_{tors}$ whenever the Tate-modules are all integrally semi-simple (and in every K-isogeny class there is such an abelian variety). Notice that assuming condition (SP) it is not true in general that there exist a K-endomorphism ϕ and a K-rational torsion point T such that $\phi(P) = Q + T$. A counterexample was found by Larsen and Schoof in [11].

5 The multilinear support problem

In this section we discuss the multilinear support problem, introduced by Barańczuk in [1]. We first show that condition (MSP) (see the Introduction) is stronger than the condition of the support problem on each pair of points.

Remark 14. Assuming condition (MSP), the following holds: for every $i = 1, \ldots, n$ the order of $(Q_i \bmod \mathfrak{p})$ divides the order of $(P_i \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

Proof. Without loss of generality it suffices to prove the claim for P_1 and Q_1. Let $\mathfrak{p}$ be a prime ideal of K such that condition (MSP) holds. For every $i \neq 1$ fix m_i such that $(m_i P_i \bmod \mathfrak{p}) = 0$ and $(m_i Q_i \bmod \mathfrak{p}) = 0$. Then for every positive integer m_1 we have $(m_1 Q_1 \bmod \mathfrak{p}) = 0$ whenever $(m_1 P_1 \bmod \mathfrak{p}) = 0$. Consequently, the order of $(Q_1 \bmod \mathfrak{p})$ divides the order of $(P_1 \bmod \mathfrak{p})$. □

Because of the previous remark and the Main Theorem, there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. One would like to prove that ϕ_i and ϕ_j are related for $i \neq j$. This is true if the endomorphism ring is $\mathbb{Z}$ (see [1]) but in general ϕ_i and ϕ_j are not related for $i \neq j$:

Example 15. Let E be an elliptic curve defined over a number field K. Let R_1, R_2 be points in $E(K)$ and let ϕ_1, ϕ_2 be in $\mathrm{End}_K E$. The following points in $E^2(K)$ satisfy condition (MSP):

$$P_1 = (R_1, 0)\,;\ P_2 = (0, R_2)\,;\ Q_1 = (\phi_1(R_1), 0)\,;\ Q_2 = (0, \phi_2(R_2)).$$

The next example shows that ϕ_i and ϕ_j are in general not related, not even for an elliptic curve, if we require the following weaker condition:

(LMSP) Fix a rational prime ℓ and suppose that for all but finitely many primes $\mathfrak{p}$ of K and for all positive integers $m_1, \ldots, m_n$ the order of $(m_1 Q_1 + \ldots + m_n Q_n \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(m_1 P_1 + \ldots + m_n P_n \bmod \mathfrak{p})$ is coprime to ℓ.

Example 16. Let E be an elliptic curve defined over a number field K such that $\mathrm{End}_K E = \mathbb{Z}[i]$. Let ϕ_1 and ϕ_2 be in $\mathrm{End}_K E$ and let P_1 be in $E(K)$. The following points satisfy condition (LMSP) for $\ell = 3$:

$$P_1\,;\ P_2 = i(P_1)\,;\ Q_1 = \phi_1(P_1)\,;\ Q_2 = \phi_2(P_2).$$

Indeed, let $\mathfrak{p}$ be a prime of K of good reduction for E and not over 3 and suppose that $(m_1 P_1 + m_2 P_2 \bmod \mathfrak{p})$ has order coprime to 3. It is clearly sufficient to show that both $(m_1 P_1 \bmod \mathfrak{p})$ and $(m_2 P_2 \bmod \mathfrak{p})$ have order coprime to 3. By multiplying P_1 and P_2 by an integer coprime to 3, we may assume that $(P_1 \bmod \mathfrak{p}) = (R \bmod \mathfrak{p})$ for a point R in $E[3^\infty]$. Then we have $(m_1 R + m_2 i(R) \bmod \mathfrak{p}) = 0$ and by the injectivity of the reduction modulo $\mathfrak{p}$ on $E[3^\infty]$ we deduce that $m_1 R + m_2 i(R) = 0$. We have to show that $m_1 R = 0$. Let 3^h be the order of R. Then the annihilator of R is an ideal of $\mathbb{Z}[i]$ containing 3^h but not 3^{h-1}. Since 3 is prime in $\mathbb{Z}[i]$, the annihilator of R is (3^h). Since $m_1 + m_2 i$ belongs to (3^h), we can write $(m_1 + m_2 i) = 3^h(a_1 + a_2 i)$ for some integers a_1, a_2. Therefore $m_1 R = 3^h a_1 R = 0$.

We can also weaken condition (MSP) by imposing that $m_1 = 1$. Then one would like to prove that for every i there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. Without loss of generality it suffices to take $n = 2$:

(WMSP) Suppose that for all but finitely many primes $\mathfrak{p}$ of K and for all positive integers m the point $(Q_1 + mQ_2 \bmod \mathfrak{p})$ is zero whenever the point $(P_1 + mP_2 \bmod \mathfrak{p})$ is zero.

If G is a simple abelian variety, under condition (WMPS) Barańczuk showed that for $i = 1, 2$ there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$, see [1, Theorem 8.1]. The same proof holds for the multiplicative group hence for 1-dimensional tori. This result is in general false for a non-simple abelian variety or for a torus of dimension > 1, as the following example shows.

Example 17. Let G be either an elliptic curve without complex multiplication or the multiplicative group defined over a number field K. Suppose that the rank of $G(K)$ is greater than 1. Then let (R, W) be a K-rational point on G^2 which is independent. Consider the following points in $G^2(K)$:

$$P_1 = Q_1 = Q_2 = (R, 0)\,; P_2 = (0, W).$$

These points satisfy condition (WMSP) but there do not exist a K-endomorphism ϕ of G^2 and a non-zero integer c such that $\phi(P_2) = cQ_2$.

Acknowledgements

I thank Brian Conrad, Marc Hindry, René Schoof for helpful discussions. I thank Jeroen Demeyer and Willem Jan Palenstijn for Example 16 and the case of 1-dimensional tori.

References

[1] S. Barańczuk, *On reduction maps and support problem in K-theory and abelian varieties*, J. Number Theory **119** (2006), no. 1, 1–17.

[2] S. Barańczuk, *On a generalization of the support problem of Erdös and its analogues for abelian varieties and K-theory*, arXiv:0809.1991v3, 2008.

[3] D. Bertrand, *Minimal heights and polarizations on abelian varieties*, preprint M.S.R.I. 06220-87, 1987.

[4] G. Banaszak, W. Gajda, and P. Krasoń, *Support problem for the intermediate Jacobians of ℓ-adic representations*, J. Number Theory **100** (2003), no. 1, 133–168.

[5] C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, J. Number Theory **64** (1997), no. 2, 276–290.

[6] C. Khare, *Compatible systems of mod p Galois representations and Hecke characters*, Math. Res. Lett. **10** (2003), no. 1, 71–83.

[7] C. Khare and D. Prasad, *Reduction of homomorphisms mod p and algebraicity*, arXiv:0211004v1, 2002.

[8] C. Khare and D. Prasad, *Reduction of homomorphisms mod p and algebraicity*, J. Number Theory **105** (2004), no. 2, 322–332.

[9] M. Larsen, *The support problem for abelian varieties*, J. Number Theory **101** (2003), no. 2, 398–403.

[10] M. Larsen and R. Schoof, *Whitehead's lemma and Galois cohomology of abelian varieties*, `http://mlarsen.math.indiana.edu/~larsen/unpublished.html`, 2004.

[11] M. Larsen and R. Schoof, *A refined counter-example to the support conjecture for abelian varieties*, J. Number Theory **116** (2006), no. 2, 396–398.

[12] M. McQuillan, *Division points on semi-abelian varieties*, Invent. math. **120** (1995), no. 1, 143–159.

[13] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. Number Theory **129** (2009), no. 2, 469–476.

[14] N. Ratazzi and E. Ullmo, *Galois + Équidistribution = Manin–Mumford*, `http://www.math.u-psud.fr/~ratazzi/recherche.html`, 2007.

[15] O. Wittenberg, *Le problème du support pour les variétés abéliennes, d'après Larsen*, `http://www.dma.ens.fr/~wittenberg/autres.html`, 2003.

Mathématiques, École Polytechnique Fédérale de Lausanne,
1015 Lausanne, Switzerland

e-mail: antonella.perucca@epfl.ch